Department of Homeland Security Daily Open Source Infrastructure Report for 23 August 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks

For info click here http://www.dhs.gov/

Daily Highlights

- The Canadian Press reports North American sales of the drug oseltamivir −− sold as Tamiflu −− have more than tripled in recent months, a trend public health experts see as evidence individuals are stockpiling the antiviral as a hedge against a possible flu pandemic. (See item 12)
- The News−Journal reports thousands of residents in Florida's Flagler County are expected to sign up for a new emergency alert notification system, that enables residents to receive timely emergency notices by cell phone, land line, pager, personal data assistant, fax, or e−mail. (See item 15)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 22, KRON 4 (CA)* — **Investigation into San Francisco transformer blast begins.** An independent outside investigator is beginning the work of trying to figure out what caused a Pacific Gas and Electric (PG&E) transformer to explode Friday, August 19, seriously injuring a woman. PG&E crews are getting organized to start inspecting all of the 540 underground vaults holding the transformers across San Francisco. The utility says it expects to have answers about what caused Friday's blast by the end of this week. Experts say it's rare for such transformers to

explode. Usually when they do a circuit overload is to blame, but PG&E officials say that did not happen in this case. The blast occurred outside the Crocker Galleria at Kearny at Post streets in San Francisco's financial district.
Source: http://www.kron4.com/Global/story.asp?S=3750639

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *August 22, CBS 3 (PA)* — **Tanker fire closes highway ramps in Pennsylvania.** A tanker truck overturned and caught fire Monday morning, August 22, on the eastbound Pennsylvania Turnpike ramp to the northbound Northeast Extension. State officials say that an early investigation indicated that high speed may be to blame for the accident. The driver, who was hauling gasoline, did not slow down enough coming around the curb onto the Northeast Extension. The driver was able to jump out of his cab just before it overturned. He was flown to the University of Pennsylvania for treatment since the extent of his injuries was not immediately known. The ramp was closed as it was overcome by smoke and flames. The eastbound turnpike ramp to the turnpike's Northeast Extension was also closed. The fire burned for nearly 30 minutes reducing the tractor−trailer to mere cinders before two large U.S. Navy foam trucks from the nearby Willow Grove Naval Air Station arrived. No word on when the ramp will be reopened.
Source: http://kyw.com/Local%20News/local_story_234093232.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *August 22, The Register (UK)* — **Air Force scrambles after privacy breach.** The U.S. Air Force has been forced to notify more than 33,000 airmen that their personal details might have been exposed following the discovery of a computer security breach. The notification comes after Air Force personnel officers discovered suspiciously high activity on one account into a careers database, called AMS (Assignment Management System), dating back to June. A preliminary investigation suggests a hacker used a legitimate user's login information to access sensitive data from servers at the Randolph Air Force Base in Texas, the headquarters of the Air Force's human resources operations. The AMS system is used for assignment preferences and career management and contains career information on officers and enlisted Airmen, as well as some personal information such as dates of birth and Social Security numbers. It does not contain personal addresses, phone numbers or information about family members. The motive for the attack remains unclear but affected air force personnel are being urged to take precautions in case their details are misused by identity thieves. Meanwhile Air Force and federal investigators are investigating the breach.

Source: http://www.theregister.co.uk/2005/08/22/air_force_privacy_br each/

4. *August 20, Colorado Daily* — **More Colorado students at risk for identity theft.** The University of Colorado has turned up another case of unauthorized access of one of its computer servers, potentially exposing 49,000 database entries that could put some current and former students at risk for identity theft. There was no evidence that personal information was stolen or used, university officials said on Friday, August 19. The affected server held ancillary information used by the Registrar's Office and has been taken offline. Information including Social Security numbers, names, addresses and phone numbers dating from June 1999 to May 2001 and from fall 2003 to summer 2005 could have been accessed, university officials said.
Source: http://www.coloradodaily.com/articles/2005/08/20/news/news04 .txt

[Return to top]

Transportation and Border Security Sector

5. *August 22, Las Vegas Business Press (NV)* — **New federal funds revive Maglev project.** The newly reauthorized federal transportation bill allocates $45 million for a super high−speed train connecting Las Vegas, NV, to Anaheim, CA, a project that was first proposed over 17 years ago. Maglev (magnetic levitation) uses high−powered magnets to propel trains above an elevated track. Since there is no friction, trains can travel up to 300 mph and climb 10 percent grades. A test track in Hamburg, Germany, would be used as a model for the proposed Las Vegas−to−Anaheim line. Now, after years of studies and millions in federal subsidies, the super−speed train could finally break ground on an initial 42−mile segment from Primm, NV, to Las Vegas as early as 2008. The lightning−quick trip would take only 18 minutes from start−to−finish. A complete journey to Southern California would last 86 minutes. Construction would cost an estimated $1.5 billion, or $35.7 million per track mile. The commission will use the $45 million federal allocation for completing an environmental impact statement. The study is a necessary step for construction to move forward. The Nevada Department of Transportation will oversee the study, which is expected to take 18 to 24 months to complete.
California−Nevada Super Speed Train Website: http://www.maglev−train.com/home.asp
The California MAGLEV Alliance Website: http://www.calmaglev.org/
Nevada Department of Transportation: http://www.nevadadot.com/
Source: http://www.lvbusinesspress.com/articles/2005/08/22/news/news 02.txt

6. *August 22, San Antonio Express−News (TX)* — **Congress to approve funding for Border Patrol agents.** Despite increased federal spending, the southern border remains porous to thousands of undocumented immigrants, and U.S. law enforcement is woefully understaffed and unable to stanch the flow, an Alabama congressman said Monday, August 22. Rep. Mike Rogers, chairman of the House Homeland Security subcommittee on management and oversight, said Congress must approve funding for additional Border Patrol agents. A bipartisan group of lawmakers, including Rep. Sheila Jackson Lee, D−Houston, spent four days along the U.S.−Mexico border to review manpower and equipment needs. The group began in El Paso and finished in Nogales, AZ. An increase in funding for new Border Patrol agents is included in the $30.8 billion spending bill for the Department of Homeland Security. Congress has authorized spending for an additional 10,000 new Border Patrol agents over the next five years. Rogers urged conferees to approve as least 1,000 of those positions in the Homeland Security

bill for fiscal year 2006, which begins October 1. In addition, Rogers said the Department of Homeland Security must work quickly to implement the $2.5 billion program that establishes infrared cameras along the border to track undocumented crossers and smugglers.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA082205.funding.online.9be67cf5.html

7. *August 22, CNN* — **'Mayday' calls from doomed Cypriot jet.** An exhausted−sounding man sent last−minute "Mayday" calls from a Cypriot airliner that mysteriously crashed earlier this month killing 121 people, investigators have revealed. But according to Greek media the calls went unheeded because the man was tuned to the wrong frequency. Police have confirmed that steward Andreas Prodromou, who was learning to fly small planes, was inside the cockpit and appeared to be trying to fly the plane for about 30 minutes before it crashed. The plane ran out of fuel at 35,000 feet after flying for nearly twice the scheduled 90 minutes from Larnaca in Cyprus to Athens, a stop on the way to its final destination, Prague. In a preliminary report released Monday, August 22, investigators said the plane appeared to suffer a depressurization problem and crashed when the engines stopped after it ran out of fuel. The Helios Airways Boeing 737 crashed on August 14 into mountains near Athens, killing all 115 passengers and six crew in Greece and Cyprus' worst air disaster. Helios, owned by Libra Holidays Group, a British holiday tour operator, has defended its record but revealed the crashed plane had a previous cabin pressure problem. Last December the plane had to descend swiftly from 34,000 to 11,000 feet on a Warsaw−Larnaca flight.
Source: http://edition.cnn.com/2005/WORLD/europe/08/22/greece.crash. mayday/

8. *August 18, Transportation Security Administration* — **PortSTEP program initiated.** The Transportation Security Administration (TSA) and the U.S. Coast Guard began a series of transportation system port security exercises on Thursday, August 18, in San Francisco. The Port Security Training Exercises Program (PortSTEP) is focused on building links within the Area Maritime Security (AMS) Committee. The committee assists the captain of the port in writing, reviewing and updating an AMS Plan in addition to supporting other transportation entities that depend upon the port being secure. The exercise will involve the entire port community, including both public governmental agencies and private industry. The partnership is intended to improve connectivity of various surface transportation modes and enhance current Area Maritime Security Plans. Scenarios range from how officials react to discovering a suspect cargo container to an explosion at a seaport rail yard. Communication and coordination abilities of the government and maritime industry will be tested at each of the 40 seaports scheduled to participate over the next three years. In addition to TSA and the U.S. Coast Guard, the Federal Highway Administration and the Maritime Administration are among participants in the PortSTEP exercise.
For more information regarding TSA, go to http://www.tsa.gov.
For more information regarding the U.S. Coast Guard, go to http://www.USCG.mil.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 015c2cd

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

9. *August 21, Middletown Press (CT)* — **Veterinarians prepare for animal disasters.** A hurricane swept through Connecticut earlier this month, cutting power to a chicken house and setting 1,000 animals loose on the streets. The mayhem was a simulation run by Middletown−based Connecticut Veterinary Medical Association (CVMA) inside a conference room. CVMA is banding together with federal agencies and universities to form the Connecticut State Animal Response Team, a group designed to respond to and prepare for animal emergencies. While Connecticut agencies have systems in place to rescue humans, CTSART members feel the state is not equipped to protect animals if hurricanes, floods, ice storms, or acts of bioterrorism sabotage the state. If another great flood hits the Connecticut River Valley, cities would lack animal−saving re−sources, said Peter Conserva, a Suffield−based equine practitioner and treasurer for the CVMA. Conserva helps steer CTSART, which is in nascent stages and will combine forces of the state Department of Emergency Management and Homeland Security, the state Department of Agriculture, the University of Connecticut and CVMA.
   CVMA Website: http://www.ctvet.org/
   State Animal Response Teams Website: http://www.sartusa.org/
   Connecticut Department of Emergency Management and Homeland Security: http://www.ct.gov/demhs/site/default.asp
   Connecticut Department of Agriculture: http://www.ct.gov/doag/site/default.asp
   University of Connecticut: http://www.uconn.edu/
   Source: http://www.middletownpress.com/site/news.cfm?newsid=15072645&BRD=1645&PAG=461&dept_id=10856&rfi=6

10. *August 21, StandardBred (Canada)* — **Eastern Equine Encephalitis found in Delaware.** A five−year−old Standardbred horse that died last August 14 in Frankford, DE, area has tested positive for Eastern Equine Encephalitis (EEE). The viral disease is spread by mosquitoes. It has a 90 percent death rate for horses. The disease is most prevalent during the months of August, September, and October. Two sentinel chickens located about five miles from where the Standardbred died also tested positively for the disease. State veterinarian H. Wesley Towers urges horse owners to contact their veterinarian and have their horses vaccinated for EEE.
    Source: http://www.standardbredcanada.ca/news/iss0805/eeedelaware082_1.html

[Return to top]

Food Sector

11. *August 19, Food Safety and Inspection Service* — **Beef products recalled.** Green Bay Dressed Beef, a Green Bay, WI, establishment, is voluntarily recalling approximately 1,856 pounds of beef products that may contain portions of the backbone from a cow just over 30 months old, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Friday, August 19. The product was from a cow imported directly for slaughter from Canada.

The products subject to this recall are from a cow that is approximately one month older than the 30−month age limit. Both ante−mortem and post−mortem inspections were done on the cow in question. FSIS inspection program personnel determined the cow to be healthy and fit for human food. FSIS learned about this as a result of a Canadian audit of their health certificate that accompanied the imported cow. Prior to slaughter, the health certificate accompanying the cow was presented to the establishment, and it appeared complete and accurate. However, a subsequent audit of information related to the health certificate by Canadian officials found that it was not accurate. The products were distributed to wholesale distributors in Pennsylvania, Florida, Illinois, Maryland, Minnesota, and Wisconsin.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_032_2005_Relea se/index.asp

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

12. *August 22, Canadian Press* — **Sales of key antiviral drug soar.** North American sales of the drug oseltamivir have more than tripled in recent months, a trend public health experts see as evidence individuals are stockpiling the antiviral as a hedge against a possible flu pandemic. "We are on a collision course to panic," warns Michael Osterholm, director of the Center for Infectious Disease Research and Policy at the University of Minnesota. "I think that what's going to happen is . . . that this drug −− which has yet to really be demonstrated to have any clinical impact on H5N1 infection −− is now going to become the I can't get product, therefore I must have it right away product. The reality is going to come through that there is only so much available." H5N1 is the avian flu strain experts fear may be poised to trigger a pandemic. Swiss drug maker Roche won't say how much oseltamivir −− sold as Tamiflu −− it can make. But the company insists individuals don't draw from the same pool as the governments placing stockpile orders. Canadian Tamiflu sales jumped to more than 76,000 prescriptions in the 12−month period ending in June, compared to 22,000 prescriptions in the entire 2004 calendar year. U.S. sales have surged to nearly 1.7 million prescriptions in the first half of 2005 from just under 500,000 in 2004.
Source: http://www.canada.com/health/story.html?id=09e47f8e−fac2−4be e−bf8a−b6936703ad17

13. *August 22, Xinhua (China)* — **Four human cases of pig−borne disease confirmed in Guangdong.** Four human cases of pig−borne disease have been reported in Guangdong, China, leaving one dead and two hospitalized. The Guangdong provincial government released the information Monday, august 22, at a provincial teleconference on prevention and control of the disease caused by swine streptococosis II bacteria. No pig cases of the disease have been reported in the province. The four human infections occured in four separate places, including the cities of Nanxiong, Shenzhen, and Yangjiang, and Chao'an County.
Source: http://news.xinhuanet.com/english/2005−08/22/content_3389675 .htm

14. *August 21, Associated Press* — **Genetic material may aid Severe Acute Respiratory Syndrome treatment.** Researchers reported Sunday, August 21, that snippets called interfering RNA can reduce an existing Severe Acute Respiratory Syndrome (SARS) infection in monkeys and help protect them from new ones. RNA transmits information from the DNA that carries the blueprint of life in cells. The fragments, called siRNA, can be tailored to silence specific genes. Researchers in China and the U.S. tested two types of siRNA that target different parts of the genome of the SARS virus. They used five groups, each with four monkeys. Two were control groups that did not receive treatment. Of the three other groups, one was treated with siRNA before being exposed to SARS; the second was treated at the same time as exposure to the disease; the third got the siRNA following infection. All the infected animals developed some symptoms. But there was much less lung damage in the animals treated with the RNA fragments. A characteristic of SARS is severe damage to the tiny air sacs in the lungs. Severe damage to those sacs was found in the control animals, while injury in the treated macaques was relatively mild, the researchers said. Throat samples taken four days after infection found evidence of the SARS virus in just 25 percent of the animals treated with siRNA.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/21/AR2005082100440.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

15. *August 22, News−Journal Online (FL)* — **Thousands in Florida county expected to sign up for new emergency alert notification system.** In the occurrence of a disaster, such as a chemical spill or a sudden tornado, Flagler County, FL, residents can now be alerted via the county's new emergency alert service, FlaglerAlert.com, which has enrolled more than 400 county residents since its June launch and expects to register thousands more. The free service enables residents to receive timely emergency notices by cell phone, land line, pager, personal data assistant, fax or e−mail, said Troy Harper, division chief of the county's emergency services department. On FlaglerAlert.com, residents can create an account, enter their name and address, and then select what information they want to know about, how they want to be contacted and the time they want to be notified. In addition to emergencies, residents can choose to be notified of road closures, county government meetings and events and programs. The system is teletypewriter compatible and can be used by the deaf and hard of hearing. With the county's population at about 70,000, officials are expecting tens of thousands to sign up.
Flagler Alert Website: http://flagleralert.com/
Source: http://www.news−journalonline.com/NewsJournalOnline/News/Flagler/03FlaglerFLAG01082205.htm

16. *August 21, The Daily Local (PA)* — **Specialized training drill held in Pennsylvania.**

Tredyffrin, PA, Lieutenant Stephen Dintino led a specialized training exercise in Chester County, PA, known as The Bus and Train Car Take−Down Tactical Action Course, Wednesday, August 17. This exercise was held to teach officers the safest and most effective way to defuse a hostage situation on a bus or train. With events such as the recent bombings in London, officers are becoming increasingly aware of the need for more specialized training, said Tredyffrin Detective Sergeant John R. Bailey. A longtime member of the Northeast Chester County Emergency Response Team (NECCERT), Bailey trains bi−weekly with Dintino and 16 other members. NECCERT includes officers from Tredyffrin, Phoenixville, Schuylkill, West Vincent and East Coventry; Wednesday's exercise included officers from West Goshen, West Chester and Westtown−East Goshen. Bailey said the point of the exercise is to eliminate the target as quickly as possible. However, in large vehicles, such as trains or buses, it may be difficult to target each hijacker, meaning officers are forced to storm the vehicle. In a scenario such as this, having a group of trained officers on the scene becomes necessary, according to Bailey.
Source: http://www.dailylocal.com/site/news.cfm?newsid=15072760&BRD=1671&PAG=461&dept_id=17782&rfi=6

17. *August 21, The Charlotte Observer (NC)* — **U.S. government wants to emulate security program.** An emergency preparedness program in Concord, NC, has succeeded well enough to catch the eye of the federal government, which is striving to replicate it. From first aid to fire safety and search and rescue, the Citizen Corps Council of Concord trains local residents for emergencies or disasters. It's been steadily gaining support from residents throughout the county. Last week, two officials from the Department of Homeland Security were sent to Concord to learn how to create similar successes across the country. Part of the program's success is due to its localized feel and the fact that many of Concord's families feel strongly rooted in the community, local officials said. Programs such as Community Emergency Response Teams (CERT) and Neighborhood Watch fall under the umbrella of the Citizen Corps Council. Concord's CERT program has trained 256 community members since it was developed in 1998, said Jim Sells, emergency management coordinator for Concord. Concord was one of five cities chosen by DHS for the study, including Detroit, Seattle, Independence, MO, and Fairfax, VA.
Source: http://www.charlotte.com/mld/observer/news/local/states/north_carolina/counties/cabarrus/12437449.htm

18. *August 20, San Francisco Chronicle (CA)* — **California city gets its first major post−September 11 disaster response system test.** The underground explosion of an electrical transformer in San Francisco, CA's, Financial District on Friday, August 19, marked the first major test of the city's post−September 11 disaster response system, and city officials said they were satisfied with the results. Mayor Gavin Newsom said city authorities alerted an assortment of federal, state and local agencies when the transformer at Kearny and Post streets blew up. Teams from the agencies worked together to secure the scene and check for bombs and dangerous chemicals that could have been spread in a terrorist attack. Other precautions included evacuating several nearby buildings and shutting down streets in the area. Pacific Gas and Electric (PG&E) officials noticed the difference since the September 11 terrorist attacks. Before September 11, said spokesperson Paul Moreno, utility crews would have gone into the transformer vault right away to check out the blast. On Friday, they had to wait while law enforcement officers combed the area for any explosive devices. Police and fire officials moved

quickly to set up a unified command post. From there, the other pieces fell into place −− buses were rerouted, streets were blocked off, rescue crews were sent in, and police secured the area.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/08/20/MNG2 KEAS051.DTL

[Return to top]

Information Technology and Telecommunications Sector

19. *August 21, FrSIRT* — **Electronic Mail for UNIX expires header buffer overflow vulnerability.** A vulnerability was identified in ELM (Electronic Mail for UNIX), which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a stack overflow error when processing specially crafted messages containing malformed "Expires" headers, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to read a specially crafted email. Products affected are Electronic Mail for UNIX (ELM) version 2.5−PL7 and prior
Users should upgrade to Electronic Mail for UNIX (ELM) version 2.5−PL8:
http://www.instinct.org/elm/files/tarballs/elm2.5.8.tar.gz
Source: http://www.frsirt.com/english/advisories/2005/1479

20. *August 21, Security Tracker* — **Land Down Under input validation bugs permit SQL injection and cross−site scripting attacks.** Some input validation vulnerabilities were reported in Land Down Under. A remote user can conduct cross−site scripting attacks. A remote user can also inject SQL commands. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Land Down Under software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can execute SQL commands on the underlying database. No solution is currently known.
Source: http://www.securitytracker.com/alerts/2005/Aug/1014747.html

21. *August 20, Security Focus* — **PCRE Regular Expression heap overflow vulnerability.** PCRE is prone to a heap overflow vulnerability. This issue is due to a failure of the library to properly bounds check user−supplied input prior to copying data to an internal memory buffer. The impact of successful exploitation of this vulnerability depends on the application and the user credentials utilizing the vulnerable library. Successful attack may ultimately permit an attacker to control the contents of critical memory control structures and write arbitrary data to arbitrary memory locations. A solution is not currently known.
Source: http://www.securityfocus.com/bid/14620/references

22. *August 19, Computer Associates* — **Computer Associates Message Queuing vulnerabilities.** There are several vulnerability issues in the Computer Associates Message Queuing (CAM / CAFT) software. The CAM TCP port is potentially vulnerable to a Denial of Service (DoS) attack; buffer overflow conditions can potentially allow arbitrary code to be executed remotely with elevated privileges; and there is potential to launch a spoof CAFT and allow arbitrary commands to be executed with elevated privileges. This affects all versions of the CA Message Queuing software prior to v1.07 Build 220_13 and v1.11 Build 29_13 on the specified platforms. Patches are available for all affected users.

Source: http://supportconnectw.ca.com/public/ca_common_docs/camsecur ity_notice.asp

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in the Microsoft DDS Library Shape Control (msdds.dll) component, which comes with various Microsoft products such as Visual Studio .NET and Microsoft Office. Systems with Visual Studio .NET 2002, which installs msdds.dll version 7.0.9466.0, are vulnerable. Based on initial testing, msdds.dll version 7.10.3077.0 does not appear vulnerable. This version of the dll is installed with Office 2003 and Visual Studio .NET 2003. Although MS Office XP provides a vulnerable version of msdds.dll, it does not appear that IE will instantiate the COM object in question with the standard installation.

By convincing a user to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the Microsoft DDS Library Shape Control COM object, a remote attacker could execute arbitrary code on the user's system with privileges of the user. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#740372 − Microsoft DDS Library Shape Control (msdds.dll) COM object contains an unspecified vulnerability

This vulnerability has similar characteristics to the previously posted javaprxy.dll vulnerability (VU#939605). The underlying vulnerability is that Internet Explorer will instantiate non−ActiveX COM objects that are referenced in an HTML document. This can cause Internet Explorer to crash. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#680526 − Microsoft Internet Explorer allows non−ActiveX COM objects to be instantiated

Until a patch is available to address this vulnerability, US−CERT strongly encourages users to review the workarounds section of Vulnerability Note (VU#740372). Additionally, Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem.

Current Port Attacks

Top 10 Target Ports	26777 (−−−), 1026 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 1433 (ms−sql−s), 135 (epmap), 21311 (−−−), 139 (netbios−ssn), 80 (www), 4672 (eMule)

Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

23. *August 22, The Plain Dealer (OH)* — **School buses get bomb checks.** Drivers from Bedford to Brunswick, OH, will sniff cargo areas and tire valves, checking for odors that could indicate a bomb. They also will look for suspicious lumps in seats, odd wires under hoods or unusual marks on fenders. State education officials say no school buses have been attacked or even threatened by bombers. But they have expanded safety checklists for bus drivers because they don't want to take chances. "This is about precaution," said J.C. Benton, a spokesperson for the Ohio Department of Education. And starting Friday, August 26, drivers will get anti−terrorism training as part of a national School Bus Watch program. The goal is to have all 20,000 of the state's bus drivers conducting security checks within two years. Topics covered by the 90−minute sessions will include a brief history of terrorism in the United States, actions and observations that drivers can take to protect themselves and children and when to report suspicious matters. The program is organized by several groups, including the National Association for Pupil Transportation, Highway Watch and the National Association of State Directors of Pupil Transportation.
Source: http://www.cleveland.com/news/plaindealer/index.ssf?/base/cuyahoga/1124703276226220.xml&coll=2

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.

Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer